Asymptotic bounds on quantum codes from algebraic geometry codes

Feng, Keqin; Ling, San; Xing, Chaoping

2006

Feng, K., Ling, S., & Xing, C. (2006). Asymptotic bounds on quantum codes from algebraic geometry codes. *IEEE Transactions on Information Theory*, 52(3), 986-991.

<https://hdl.handle.net/10356/96427>

<https://doi.org/10.1109/TIT.2005.862086>

© 2006 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/TIT.2005.862086>].

Downloaded on 26 Apr 2023 21:42:49 SGT

Asymptotic Bounds on Quantum Codes From Algebraic Geometry Codes

Keqin Feng, San Ling, and Chaoping Xing

Abstract—We generalize a characterization of p -ary (p is a prime) quantum codes given by Feng and Xing to q -ary (q is a prime power) quantum codes. This characterization makes it possible to convert an asymptotic bound of Stichtenoth and Xing for nonlinear algebraic geometry codes to a quantum asymptotic bound. Besides, we also investigate the asymptotic behavior of quantum codes.

Index Terms—Algebraic-geometry codes, asymptotic behavior, propagation rules.

I. INTRODUCTION

AS in classical coding theory, one wonders how a good family of quantum codes performs when the length tends to infinity. By linear programming methods, some asymptotic upper bounds have previously been derived (see [2]).

The first asymptotic lower bound is given in [3] using algebraic-geometry codes. This bound was improved later in [5], [9]. All these three bounds are concerned with binary quantum codes and they are far away from some reasonable upper bounds. In [1], the asymptotic quantum Gilbert–Varshamov bound is given (the finite version of the quantum Gilbert–Varshamov bound is derived in [6]). This asymptotic Gilbert–Varshamov bound for binary quantum codes is much better than those from algebraic-geometry codes. However, as in classical coding theory, the quantum Gilbert–Varshamov bound can be improved by algebraic-geometry codes using the stabilizer methods or other constructions (see Theorems 3.6 and 3.8).

In this paper, we first generalize a characterization of quantum codes from the p -ary case (p is a prime) to the q -ary case (q is a prime power) in Section II. After that, we give a construction of quantum codes from classical codes and derive some propagation rules by making use of this characterization.

In Section III, we first discuss the asymptotic behavior of quantum codes and then apply classical algebraic-geometry codes to derive the asymptotic quantum algebraic-geometry

bound using the construction in Section II (or the stabilizer method). Finally, we derive one of the main results in this paper, i.e., we employ the construction in Section II to derive an asymptotic lower bound improving the asymptotic quantum algebraic-geometry bound (the same improvement has been done recently in classical coding theory [16]). It seems that this improvement cannot be obtained from additive quantum codes.

II. A CHARACTERIZATION OF QUANTUM CODES

Binary quantum codes have been generalized to the q -ary quantum codes with q being a power of a prime [1]. First we recall the definition of q -ary quantum codes. Throughout this section, we assume that $q = p^m$ for a prime p and an integer $m \geq 1$.

Let $\mathbb{C}^q$ be a complex vector space of dimension q and $\{|a\rangle : a \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$ with respect to the Hermitian inner product $\langle \cdot, \cdot \rangle_H$ (or $\langle \cdot | \cdot \rangle$). A q -ary quantum state $|v\rangle$ is a nonzero vector in $\mathbb{C}^q$

$$0 \neq |v\rangle = \sum_{c \in \mathbb{F}_q} \alpha_c |c\rangle \quad (\alpha_c \in \mathbb{C})$$

where $\mathbb{F}_q$ denotes the finite field with q elements.

For $n \geq 1$, the n th tensor product $(\mathbb{C}^q)^{\otimes n} = \mathbb{C}^{q^n}$ has a basis $\{|c\rangle = |c_1\rangle \otimes |c_2\rangle \otimes \cdots \otimes |c_n\rangle : c = (c_1, \dots, c_n) \in \mathbb{F}_q^n\}$. A q -ary n -system state $|v\rangle$ is a nonzero vector in $(\mathbb{C}^q)^{\otimes n}$

$$0 \neq |v\rangle = \sum_{c \in \mathbb{F}_q^n} \alpha_c |c\rangle$$

where $\alpha_c \in \mathbb{C}$.

Let ζ be the p th primitive root of unity: $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$. Let δ_{ij} be the Kronecker symbol and define two $p \times p$ matrices $T = (t_{ij})$, $R = (r_{ij})$ with $t_{ij} = \delta_{i, j-1 \bmod p}$ and $r_{ij} = \zeta^i \delta_{ij}$.

Fix a basis $\{\alpha_1, \dots, \alpha_m\}$ of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$. For two elements $a = \sum_{i=1}^m a_i \alpha_i$ and $b = \sum_{i=1}^m b_i \alpha_i$, consider the error operator

$$T_a R_b = T^{a_1} R^{b_1} \otimes T^{a_2} R^{b_2} \otimes \cdots \otimes T^{a_m} R^{b_m}.$$

Then we have

$$(T_a R_b)(T_c R_d) = \zeta^{-\langle b, c \rangle} T_{a+c} R_{b+d}$$

where $\langle \cdot, \cdot \rangle$ stands for the usual inner product of $\mathbb{F}_q \simeq \mathbb{F}_p^m$ over $\mathbb{F}_p$ with respect to the basis $\{\alpha_1, \dots, \alpha_m\}$, and

$$(T_a R_b)(T_c R_d) = \zeta^{\langle a, d \rangle - \langle b, c \rangle} (T_c R_d)(T_a R_b).$$

The action of $T_a R_b$ on a basis element $|c\rangle$ of $\mathbb{C}^q$ with $c \in \mathbb{F}_q$ is as follows:

$$T_a R_b |c\rangle = \zeta^{\langle b, c \rangle} |c - a\rangle.$$

Now for two vectors

$$\mathbf{a} = (a^{(1)}, a^{(2)}, \dots, a^{(n)}) \quad \text{and} \quad \mathbf{b} = (b^{(1)}, b^{(2)}, \dots, b^{(n)})$$

K. Feng is with the Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China (e-mail: kfeng@math.tsinghua.edu.cn).

S. Ling is with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637616, Republic of Singapore (e-mail: lingsan@ntu.edu.sg).

C. Xing is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: matxcp@nus.edu.sg).

Communicated by A. E. Ashikhmin, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.862086

in $\mathbb{F}_q^n$, we define the error operator on $(\mathbb{C}^q)^{\otimes n}$ by

$$E_{\mathbf{ab}} = T_{a(1)}R_{b(1)} \otimes T_{a(2)}R_{b(2)} \otimes \cdots \otimes T_{a(n)}R_{b(n)}.$$

The set of all quantum errors

$$\mathcal{E} := \{\zeta^\lambda E_{\mathbf{ab}} : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, \lambda \in \mathbb{F}_p\}$$

forms a non-Abelian group of order p^{2mn+1} under the group law

$$E_{\mathbf{ab}}E_{\mathbf{uv}} = \zeta^{-\langle \mathbf{b}, \mathbf{u} \rangle} E_{\mathbf{a+u}}E_{\mathbf{b+v}}$$

where $\langle \mathbf{b}, \mathbf{u} \rangle = \sum_{i=1}^n \langle b^{(i)}, u^{(i)} \rangle$.

It is easy to verify that the center $C(\mathcal{E})$ of $\mathcal{E}$ is $\{\zeta^\lambda I : \lambda \in \mathbb{F}_p\}$.

The quantum weight of $E_{\mathbf{ab}}$ is defined by

$$w_Q(E_{\mathbf{ab}}) = \#\{i : 1 \leq i \leq n, (a^{(i)}, b^{(i)}) \neq (0, 0) \in \mathbb{F}_q^2\}.$$

Definition 2.1: A complex subspace $Q \neq \{0\}$ of $(\mathbb{C}^q)^{\otimes n} = \mathbb{C}^{q^n}$ is called a q -ary quantum code of length n .

We denote by $K = \dim_{\mathbb{C}} Q$ the dimension of Q over $\mathbb{C}$ and put $k = \log_q K$. Then k is a real number and $0 \leq k \leq n$.

The minimum distance of a quantum code Q is defined to be the largest positive integer d satisfying the following condition:

for any $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$ in Q with $\langle \mathbf{u} | \mathbf{v} \rangle = 0$ and $\mathbf{e} \in \mathcal{E}$ with quantum weight $\leq d-1$, we have $\langle \mathbf{u} | \mathbf{e} | \mathbf{v} \rangle = 0$.

A q -ary quantum code Q with length n , dimension K ($k = \log_q K$), and minimum distance d is denoted by $((n, K, d))_q$ or $[[n, k, d]]_q$. A quantum $((n, K, d))_q$ -code Q is called *pure* if $\langle \mathbf{u} | \mathbf{e} | \mathbf{v} \rangle = 0$ for all $\mathbf{e} \in \mathcal{E}$ with $1 \leq w_Q(\mathbf{e}) \leq d-1$ and $\mathbf{u}, \mathbf{v} \in Q$ (note that we do not require $\langle \mathbf{u} | \mathbf{v} \rangle = 0$ here).

Now we present a characterization on a quantum $((n, K, d))_q$ -code Q . It gives an alternative way to construct quantum codes.

An n -system state $|\mathbf{v}\rangle = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \alpha_{\mathbf{c}} |\mathbf{c}\rangle$ can be identified with a mapping $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{C}$ defined by $\varphi(\mathbf{c}) = \alpha_{\mathbf{c}}$ for all $\mathbf{c} \in \mathbb{F}_q^n$.

For a map $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{C}$ and a partition $\{1, 2, \dots, n\} = A \cup B$, we denote $\varphi(\mathbf{c})$ by $\varphi(\mathbf{c}_A, \mathbf{c}_B)$, where $\mathbf{c}_A$ and $\mathbf{c}_B$ are the subvectors of $\mathbf{c}$ coordinated by A and B , respectively. For two maps $\varphi, \psi : \mathbb{F}_q^n \rightarrow \mathbb{C}$, we define their hermitian inner product by

$$(\varphi, \psi) = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \overline{\varphi(\mathbf{c})} \psi(\mathbf{c}) \in \mathbb{C}$$

where $\overline{\varphi(\mathbf{c})}$ stands for the conjugate of the complex number $\varphi(\mathbf{c})$.

Theorem 2.2: There exists a quantum $((n, K, d))_q$ -code with $K \geq 2$ if and only if there exist K nonzero mappings

$$\varphi_i : \mathbb{F}_q^n \rightarrow \mathbb{C} \quad (1 \leq i \leq K) \quad (2.1)$$

satisfying the following condition:

for each partition $\{1, 2, \dots, n\} = A \cup B$ with $|A| = d-1$ and $|B| = n-d+1$, and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_q^{d-1}$, $1 \leq i, j \leq n$,

$$\sum_{\mathbf{c}_B \in \mathbb{F}_q^{n-d+1}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_B) = \begin{cases} 0, & \text{if } 1 \leq i \neq j \leq K \\ f, & \text{if } 1 \leq i = j \leq K \end{cases} \quad (2.2)$$

where f is independent of i and depends only on $\mathbf{c}_A$ and $\mathbf{c}'_A$.

Proof: Let Q be a K -dimensional subspace of $\mathbb{C}^{q^n}$ with an orthonormal basis

$$|\mathbf{v}_i\rangle = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \varphi_i(\mathbf{c}) |\mathbf{c}\rangle \quad (1 \leq i \leq K)$$

i.e.,

$$(\varphi_i, \varphi_j) = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \overline{\varphi_i(\mathbf{c})} \varphi_j(\mathbf{c}) = \langle \mathbf{v}_i | \mathbf{v}_j \rangle = \begin{cases} 0, & \text{if } i \neq j \\ 1, & \text{if } i = j. \end{cases}$$

For two vectors in Q

$$|\mathbf{u}\rangle = \sum_{i=1}^K \alpha_i |\mathbf{v}_i\rangle, \quad |\mathbf{u}'\rangle = \sum_{i=1}^K \alpha'_i |\mathbf{v}_i\rangle \quad (\alpha_i, \alpha'_i \in \mathbb{C})$$

we have

$$\langle \mathbf{u} | \mathbf{u}' \rangle = \sum_{i,j=1}^K \overline{\alpha_i} \alpha'_j \langle \mathbf{v}_i | \mathbf{v}_j \rangle = \sum_{i=1}^K \overline{\alpha_i} \alpha'_i. \quad (2.3)$$

For each $\mathbf{e} = E_{\mathbf{ab}}$, $w_Q(\mathbf{e}) = l$, let

$$A = \{i \mid 1 \leq i \leq n, (a^{(i)}, b^{(i)}) \neq (0, 0)\}.$$

Then we have a partition $\{1, 2, \dots, n\} = A \cup B$ with $|A| = l$, $|B| = n-l$, and $\mathbf{e} = E_{(\mathbf{a}_A, \mathbf{0}_B), (\mathbf{b}_A, \mathbf{0}_B)}$. Thus,

$$\begin{aligned} \langle \mathbf{u} | \mathbf{u}' \rangle &= \sum_{j=1}^K \alpha'_j \langle \mathbf{u} | \mathbf{v}_j \rangle = \sum_{j=1}^K \alpha'_j \sum_{\mathbf{c} \in \mathbb{F}_q^n} \varphi_j(\mathbf{c}) \langle \mathbf{u} | \mathbf{c} \rangle \\ &= \sum_{j=1}^K \alpha'_j \sum_{\mathbf{c} \in \mathbb{F}_q^n} \varphi_j(\mathbf{c}) \zeta^{\langle \mathbf{b}, \mathbf{c} \rangle} |\mathbf{c} - \mathbf{a}\rangle \\ &= \sum_{j=1}^K \alpha'_j \sum_{\mathbf{c}_A \in \mathbb{F}_q^l, \mathbf{c}_B \in \mathbb{F}_q^{n-l}} \varphi_j(\mathbf{c}_A, \mathbf{c}_B) \zeta^{\langle \mathbf{b}_A, \mathbf{c}_A \rangle} |\mathbf{c}_A - \mathbf{a}_A, \mathbf{c}_B\rangle \\ &= \sum_{j=1}^K \alpha'_j \sum_{\mathbf{c}_A, \mathbf{c}_B} \zeta^{\langle \mathbf{b}_A, (\mathbf{c}_A - \mathbf{a}_A) \rangle} \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_B) |\mathbf{c}_A, \mathbf{c}_B\rangle. \end{aligned}$$

Therefore,

$$\langle \mathbf{u} | \mathbf{e} | \mathbf{u}' \rangle = \sum_{i,j=1}^K \overline{\alpha_i} \alpha'_j \sum_{\mathbf{c}_A, \mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_B) \zeta^{\langle \mathbf{b}_A, \mathbf{c}_A \rangle}. \quad (2.4)$$

By definition, Q is a quantum code with minimum distance d if and only if $\langle \mathbf{u} | \mathbf{e} | \mathbf{u}' \rangle = 0$ for any orthogonal $|\mathbf{u}\rangle$ and $|\mathbf{u}'\rangle$ in Q and $\mathbf{e}$ of quantum weight $\leq d-1$. It follows from (2.3) and (2.4) that this is equivalent to the following:

for each partition $\{1, 2, \dots, n\} = A \cup B$ with $|A| = d-1$, $|B| = n-d+1$, $\mathbf{a}_A, \mathbf{b}_A \in \mathbb{F}_q^{d-1}$ and $\sum_{i=1}^K \overline{\alpha_i} \alpha'_j = 0$ implies that

$$\sum_{i,j=1}^K \overline{\alpha_i} \alpha'_j \sum_{\mathbf{c}_A, \mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_B) \zeta^{\langle \mathbf{b}_A, \mathbf{c}_A \rangle} = 0. \quad (2.5)$$

By the Fourier transformation, the condition (2.5) is equivalent to

$$\sum_{i,j=1}^K \overline{\alpha_i} \alpha'_j \sum_{\mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_B) = 0 \quad (2.6)$$

for each partition $\{1, 2, \dots, n\} = A \cup B$ with $|A| = d - 1$, $|B| = n - d + 1$ and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_p^{d-1}$. Let

$$M = (m_{ij})_{1 \leq i, j \leq K}, \quad m_{ij} = \sum_{\mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_B) \in \mathbb{C}.$$

Our condition becomes that for any $\alpha, \alpha' \in \mathbb{C}^K$ with $\langle \alpha, \alpha' \rangle_H = 0$ implies that $\overline{\alpha} M \alpha'^T = 0$. It is easy to see that under the assumption $K \geq 2$, the condition is equivalent to $M \alpha'^T = f \alpha'^T$ for any $\alpha' \in \mathbb{C}^K$, where $f \in \mathbb{C}$ is independent of α' . Thus, $M = f I_K$. This implies that our condition is equivalent to the condition (2.2). $\square$

Using the above characterization of quantum codes, we are now able to give a construction of quantum codes from classical codes.

Lemma 2.3: Let C be a classical q -ary $[n, k]$ -linear code. If the minimum distance $d(C^\perp)$ of the dual code is at least d , then for each partition $\{1, 2, \dots, n\} = A \cup B$ with $|A| = d - 1$ and $|B| = n - d + 1$, and any $\mathbf{c}_A \in \mathbb{F}_q^{d-1}$ and $\mathbf{v} \in \mathbb{F}_q^n$, one has

$$\#\{\mathbf{c}_B \in \mathbb{F}_q^{n-d+1} : (\mathbf{c}_A, \mathbf{c}_B) \in \mathbf{v} + C\} = q^{k-d+1}.$$

Proof: This result is a well-known fact about the relationship between linear codes and orthogonal arrays. It says that if C is a classical q -ary $[n, k]$ -linear code and the minimum distance $d(C^\perp)$ of the dual code is at least d , then any coset of C is an orthogonal array of level q and strength $d - 1$ (see [8, Theorem 4.6]). $\square$

Proposition 2.4: Let C be a q -ary classical linear code of length n and $V = \{\mathbf{v}_i\}_{i=1}^K$ be a set of K distinct vectors in $\mathbb{F}_q^n$. Put

$$d_v := \min\{\text{wt}(\mathbf{v}_i - \mathbf{v}_j + \mathbf{c}) : 1 \leq i \neq j \leq K \text{ and } \mathbf{c} \in C\}$$

and $d = \min\{d_v, d(C^\perp)\}$, where wt denotes the Hamming weight. If $d > 0$, then we have a q -ary $((n, K, d))$ -quantum code.

Proof: For each $1 \leq i \leq K$, define a mapping $\varphi_i : \mathbb{F}_q^n \rightarrow \mathbb{C}$ given by

$$\mathbf{u} \mapsto \begin{cases} 1, & \text{if } \mathbf{u} \in \mathbf{v}_i + C \\ 0, & \text{if } \mathbf{u} \notin \mathbf{v}_i + C. \end{cases}$$

Next we have to verify that the condition (2.2) in Theorem 2.2 is satisfied.

For each partition $\{1, 2, \dots, n\} = A \cup B$ with $|A| = d - 1$ and $|B| = n - d + 1$, and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_q^{d-1}$

$$\overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_i(\mathbf{c}'_A, \mathbf{c}_B) \neq 0$$

if and only if

$$\varphi_i(\mathbf{c}_A, \mathbf{c}_B) = \varphi_i(\mathbf{c}'_A, \mathbf{c}_B) = 1$$

i.e., $(\mathbf{c}_A, \mathbf{c}_B), (\mathbf{c}'_A, \mathbf{c}_B) \in \mathbf{v}_i + C$. This is equivalent to

$$(\mathbf{c}_A - \mathbf{c}'_A, \mathbf{0}) \in C \quad \text{and} \quad (\mathbf{c}_A, \mathbf{c}_B) \in \mathbf{v}_i + C. \quad (2.7)$$

By Lemma 2.3 and the condition (2.7), we have

$$\begin{aligned} \sum_{\mathbf{c}_B \in \mathbb{F}_q^{n-d+1}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_i(\mathbf{c}'_A, \mathbf{c}_B) \\ = \begin{cases} 0, & \text{if } (\mathbf{c}_A - \mathbf{c}'_A, \mathbf{0}) \notin C \\ q^{k-d+1}, & \text{if } (\mathbf{c}_A - \mathbf{c}'_A, \mathbf{0}) \in C \end{cases} \end{aligned}$$

If $1 \leq i \neq j \leq K$, we must have that $(\mathbf{c}_A - \mathbf{c}'_A, \mathbf{0}) \notin \mathbf{v}_i - \mathbf{v}_j + C$ since $\text{wt}(\mathbf{c}_A - \mathbf{c}'_A, \mathbf{0}) \leq d - 1 < d \leq \text{wt}(\mathbf{v}_i - \mathbf{v}_j + C)$. This implies that either $(\mathbf{c}_A, \mathbf{c}_B) \notin \mathbf{v}_i + C$ or $(\mathbf{c}_A, \mathbf{c}_B) \notin \mathbf{v}_j + C$ for any fixed $\mathbf{c}_B$. Hence, $\overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_B) = 0$ for any fixed $\mathbf{c}_B$ and thus,

$$\sum_{\mathbf{c}_B \in \mathbb{F}_q^{n-d+1}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_B) = 0.$$

This completes the proof. $\square$

Corollary 2.5: Assume that we have two q -ary classical linear codes $[n, k_i]$ ($i = 1, 2$) such that $C_1 \subset C_2$. Then there exists a q -ary $((n, K, d))$ -quantum code with $K = q^{k_2 - k_1}$ and $d = \min\{d(C_2), d(C_1^\perp)\}$.

Proof: Let $\mathbf{v}_1, \dots, \mathbf{v}_K$ be elements of C_2 such that $\mathbf{v}_1 + C_1, \dots, \mathbf{v}_K + C_1$ are K distinct cosets of C_1 . Putting $C = C_1$ and applying Proposition 2.4, we obtain the desired result. $\square$

Remark 2.6: The result of Corollary 2.5 can be derived from stabilizer codes [4] as well. However, we will see that Proposition 2.4 can give better quantum codes than the stabilizer codes by employing classical nonlinear codes.

Example 2.7: Let $C = \{\mathbf{0}, \mathbf{1}\}$ be the binary $[n, 1, n]$ -code with $n \geq 4$. Then its dual code is a binary $[n, n - 1, 2]$ -code. Define V to be the subset $\mathbb{F}_2^n$ as follows.

Case 1. n is even.

$$V := \{\mathbf{v} \in \mathbb{F}_2^n : \text{wt}(\mathbf{v}) = (n - 2)/2 - 2i \text{ for some } 0 \leq i \leq (n - 2)/4\}.$$

Then $|V| = 2^{n-2}$.

Case 2. n is odd.

$$V := \{\mathbf{v} \in \mathbb{F}_2^n : \text{wt}(\mathbf{v}) = (n - 3)/2 - 2i \text{ for some } 0 \leq i \leq (n - 3)/4\}.$$

Then $|V| = 2^{n-2} - \frac{1}{2} \binom{n-1}{(n-1)/2}$.

It is clear that $\text{wt}(\mathbf{u} - \mathbf{v} + \mathbf{c}) \geq 2$ for any two distinct $\mathbf{u}, \mathbf{v} \in V$ and $\mathbf{c} \in C$. By Proposition 2.4, we get a binary $((n, |V|, 2))$ -quantum code, i.e., we have a binary $((n, 2^{n-2}, 2))$ -quantum code for any even $n \geq 4$ and a binary $((n, 2^{n-2} - \frac{1}{2} \binom{n-1}{(n-1)/2}, 2))$ -quantum code for any odd $n \geq 5$. Codes with the same parameters are presented in [7] as well.

In [7], we give some propagation rules. These propagation rules play a key role on determining the asymptotic behavior of quantum codes. We state these propagation rules without detailed proof.

Proposition 2.8: Suppose there is a q -ary $((n, K, d))$ -quantum code. Then

- i) **(subcode)** there exists a q -ary $((n, K - 1, \geq d))$ -quantum code;
- ii) **(lengthening)** there exists a q -ary $((n + 1, K, \geq d))$ -quantum code;
- iii) **(puncturing)** there exists a q -ary $((n - 1, K, \geq d - 1))$ -quantum code;
- iv) there exists a q -ary $((n, K, d - 1))$ -quantum code.

Proof: By Theorem 2.2, a q -ary $((n, K, d))$ -quantum code can be identified with a set $\{\varphi_i\}_{i=1}^K$ of nonzero mappings from $\mathbb{F}_q^n$ to $\mathbb{C}$ satisfying the condition (2.2).

- i) If we throw φ_K away, then it is easy to verify that the set $\{\varphi_i\}_{i=1}^{K-1}$ gives a q -ary $((n, K-1, \geq d))$ -quantum code.
- ii) For each $1 \leq i \leq K$, define a mapping

$$\theta_i : \mathbb{F}_q^{n+1} \rightarrow \mathbb{C};$$

$$(x_1, \dots, x_n, x_{n+1}) \mapsto \varphi_i(x_1, \dots, x_n).$$

Then the set $\{\theta_i\}_{i=1}^K$ defines a q -ary $((n+1, K, \geq d))$ -quantum code.

- iii) As φ_i is not identical to zero, there exists an element $\mathbf{a}_i = (a_1^{(i)}, \dots, a_n^{(i)}) \in \mathbb{F}_q^n$ such that $\varphi_i(\mathbf{a}_i) \neq 0$. Define a new mapping

$$\phi_i : \mathbb{F}_q^{n-1} \rightarrow \mathbb{C};$$

$$(x_1, \dots, x_{n-1}) \mapsto \varphi_i(x_1, \dots, x_{n-1}, a_n^{(i)})$$

for all $1 \leq i \leq K$. Then the set $\{\phi_i\}_{i=1}^K$ defines a q -ary $((n-1, K, d-1))$ quantum code.

- iv) This is clear. $\square$

III. ASYMPTOTIC BOUNDS FROM ALGEBRAIC-GEOMETRY CODES

For a q -ary quantum code Q , we denote by $n(Q)$, $K(Q)$, and $d(Q)$ the length, the dimension over $\mathbb{C}$, and the minimum distance of Q , respectively. Let U_q^Q be the set of ordered pairs $(\delta, R) \in \mathbb{R}^2$ for which there exists a family $\{Q_i\}_{i=1}^\infty$ of q -ary codes with $n(Q_i) \rightarrow \infty$ and

$$\delta = \lim_{i \rightarrow \infty} \frac{d(Q_i)}{n(Q_i)}, \quad R = \lim_{i \rightarrow \infty} \frac{\log_q K(Q_i)}{n(Q_i)}$$

where $\log_q$ denotes the logarithm to the base q . One of the central asymptotic problems for quantum codes is to determine the domain U_q^Q . As in classical coding, it is a hard problem to determine U_q^Q completely. Instead, we are satisfied with some bounds on U_q^Q . First, we give a general description on the domain U_q^Q .

Proposition 3.1: There exists a function $\alpha_q^Q(\delta)$, $\delta \in [0, 1]$, such that U_q^Q is the union of the domain

$$\{(\delta, R) \in \mathbb{R}^2 : 0 \leq R < \alpha_q^Q(\delta), 0 \leq \delta \leq 1\}$$

with some points on the boundary $\alpha_q^Q(\delta)$. Moreover, $\alpha_q^Q(0) = 1$, $\alpha_q^Q(\delta) = 0$ for $\delta \in [1/2, 1]$, and $\alpha_q^Q(\delta)$ decreases on the interval $[0, 1]$.

Proof: Assume that (δ, R) is a point in U_q^Q , i.e., there exists a family $\{Q_i\}_{i=1}^\infty$ of q -ary quantum codes such that $n(Q_i) \rightarrow \infty$ as i tends to ∞ and

$$\delta = \lim_{i \rightarrow \infty} \frac{d(Q_i)}{n(Q_i)}, \quad R = \lim_{i \rightarrow \infty} \frac{\log_q K(Q_i)}{n(Q_i)}.$$

Let $0 \leq r < R$ be a real number and put

$$K_i = \left\lfloor \frac{K(Q_i)}{q^{(R-r)n(Q_i)}} \right\rfloor.$$

Then, $K_i \leq K(Q_i)$ and $(\log_q K_i)/n(Q_i) \rightarrow r < R$. By Proposition 2.8 i), there exists a family of q -ary $((n(Q_i), K_i, d(Q_i)))$ -quantum codes. Thus, (δ, r) is also a

point in U_q^Q . This implies the existence of such a function $\alpha_q^Q(\delta)$.

By the similar arguments and using Proposition 2.8 iv), we can show that (σ, R) is also a point in U_q^Q for any $0 \leq \sigma < \delta$. This shows that $\alpha_q^Q(\delta)$ is a decreasing function.

For any n , we have a trivial $((n, q^n, 1))$ -quantum code, thus $(0, 1)$ is a point in U_q^Q . Since $\alpha_q^Q(\delta) \leq 1$ for any $0 \leq \delta \leq 1$, we have $\alpha_q^Q(0) = 1$.

By the Singleton bound, we have $K \leq q^{n-2d+2}$ for any q -ary quantum codes. Hence, $\alpha_q^Q(\delta) = 0$ if $\delta \geq 1/2$. $\square$

Remark 3.2:

- i) From Proposition 3.1, determination of the domain U_q^Q is almost equivalent to determining the function $\alpha_q^Q(\delta)$.
- ii) In classical coding, the boundary $\alpha_q(\delta)$ is in the domain U_q and the function $\alpha_q(\delta)$ is continuous (see [17]). However, we do not know whether the same result holds for quantum codes. This is due to the lack of one propagation rule for quantum codes, namely, the existence of a q -ary $((n, K, d))$ -quantum code does not ensure the existence of a q -ary $((n-1, \lceil K/q \rceil, d))$ -quantum code (however, it is true that, in classical coding theory, the existence of a q -ary (n, K, d) -code implies the existence of a q -ary $(n-1, \lceil K/q \rceil, d)$ -code).

The first lower bound on $\alpha_q^Q(\delta)$ was derived in [3] using algebraic-geometry codes and later, this bound was improved by Chen–Ling–Xing [5] and Matsumoto [9]. A very good existence lower bound for p -ary quantum codes was introduced by Ashikhmin and Knill [1]. It is called the quantum Gilbert–Varshamov bound. The finite version of the q -ary quantum Gilbert–Varshamov bound was given by Feng and Ma in [6], and the asymptotic version of q -ary quantum codes can be derived easily from this finite version. As in classical coding theory, the quantum Gilbert–Varshamov bound is a benchmark for the function $\alpha_q^Q(\delta)$.

For $0 < \delta < 1$, define the q -ary entropy function

$$H_q(\delta) := \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q(1-\delta)$$

and put

$$R_{GV}(q, \delta) := 1 - \delta \log_q(q+1) - H_q(\delta).$$

The Gilbert–Varshamov bound says that

$$\alpha_q^Q(\delta) \geq R_{GV}(q, \delta), \quad \text{for all } \delta \in (0, \frac{1}{2}). \quad (3.1)$$

For $q = 2$, the Gilbert–Varshamov bound is much better than the constructive bounds given in [3], [5], [9] from algebraic-geometry codes. However, the situation is quite similar to the one in classical coding theory, i.e., for large q , the q -ary quantum Gilbert–Varshamov bound can be improved by the algebraic-geometry bound as shown below.

Before proceeding to the algebraic-geometry bounds, we recall some background on classical algebraic-geometry codes.

Let $\mathcal{X}/\mathbb{F}_q$ be an algebraic curve of genus g . We denote by $\mathbb{F}_q(\mathcal{X})$ the function field of $\mathcal{X}$. An element of $\mathbb{F}_q(\mathcal{X})$ is called a function. We write ν_P for the normalized discrete valuation corresponding to the point P of $\mathcal{X}/\mathbb{F}_q$.

For a divisor G , we form the vector space

$$\mathcal{L}(G) = \{x \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} : \text{div}(x) + G \geq 0\} \cup \{0\}.$$

Then $\mathcal{L}(G)$ is a finite-dimensional vector space over $\mathbb{F}_q$, and we denote its dimension by $\ell(G)$. By the Riemann–Roch theorem we have

$$\ell(G) \geq \deg(G) + 1 - g$$

and equality holds if $\deg(G) \geq 2g - 1$.

Let $\mathcal{P}$ be a subset of $\mathcal{X}(\mathbb{F}_q)$ and label the points in $\mathcal{P}$ as follows:

$$\mathcal{P} = \{P_1, P_2, \dots, P_n\}.$$

Choose a divisor G such that $\text{Supp}(G) \cap \mathcal{P} = \emptyset$. Then $\nu_{P_i}(f) \geq 0$ for all $1 \leq i \leq n$ and any $f \in \mathcal{L}(G)$.

Consider the map

$$\phi : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n, \quad f \mapsto (f(P_1), f(P_2), \dots, f(P_n)).$$

Then the image of ϕ forms a subspace of $\mathbb{F}_q^n$ that was defined as an algebraic-geometry code by Goppa. The image of ϕ is denoted by $C_L(G; \mathcal{P})$. If n is bigger than the degree of G , then ϕ is an embedding and the dimension k of $C_L(G; \mathcal{P})$ is equal to $\ell(G)$. The Riemann–Roch theorem makes it possible to estimate the parameters of the code $C_L(G; \mathcal{P})$.

Proposition 3.3 (See [17, Theorem 3.1.1]): Let $\mathcal{X}/\mathbb{F}_q$ be an algebraic curve of genus g and let $\mathcal{P}$ be a set of n points on $\mathcal{X}$. Choose a divisor G with $g \leq \deg(G) < n$ and $\text{Supp}(G) \cap \mathcal{P} = \emptyset$. Then $C_L(G; \mathcal{P})$ is an $[n, k, d]$ -linear code over $\mathbb{F}_q$ with

$$k \geq \deg(G) - g + 1, \quad d \geq n - \deg(G).$$

Moreover, the dimension k is equal to $\deg(G) - g + 1$ if $\deg(G) \geq 2g - 1$. Furthermore, the minimum distance $d(C_L^\perp(G; \mathcal{P}))$ of its dual code is at least $\deg(G) - 2g + 2$.

Proposition 3.4: If there is an algebraic curve $\mathcal{X}/\mathbb{F}_q$ with at least $n + 1$ points and genus g , then one has a q -ary $((n, q^{n-2m+2g-2}, m - 2g + 2))$ -quantum code for any $2g - 2 < m < n < 2m - 2g + 2$.

Proof: Let $P_0, P_1, \dots, P_n$ be $n+1$ distinct rational points of $\mathcal{X}$. Putting $\mathcal{P} = \{P_1, \dots, P_n\}$, $C_1 = C_L(mP_0, \mathcal{P})$, and $C_2 = C_L((n - m + 2g - 2)P_0, \mathcal{P})$, and applying Corollary 2.5, we obtain the desired result. $\square$

Remark 3.5: If $\mathcal{X}/\mathbb{F}_q$ is the projective line, i.e., $g = 0$, then we get q -ary $((n, q^{n-2m-2}, m + 2))$ -quantum codes for any $-1 < m < n - 1$. This class of quantum codes achieves the quantum Singleton bound.

Let $N(\mathcal{X})$ denote the number of $\mathbb{F}_q$ -rational points of a curve $\mathcal{X}/\mathbb{F}_q$ of genus $g(\mathcal{X})$. According to the Weil bound

$$N(\mathcal{X}) \leq q + 1 + 2g(\mathcal{X})\sqrt{q}$$

the following two definitions make sense.

For any prime power q and any integer $g \geq 0$, put

$$N_q(g) := \max N(\mathcal{X})$$

where the maximum is extended over all curves $\mathcal{X}/\mathbb{F}_q$ with $g(\mathcal{X}) = g$.

We also define the following asymptotic quantity:

$$A(q) := \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g}.$$

We know from [17] that $A(q) = \sqrt{q} - 1$ if q is a square.

Theorem 3.6: For a prime power q , one has

$$\alpha_q^Q(\delta) \geq 1 - 2\delta - \frac{2}{A(q)}. \quad (3.2)$$

Proof: Let $\{\mathcal{X}/\mathbb{F}_q\}$ be a family of curves such that $g(\mathcal{X}) \rightarrow \infty$ and

$$\limsup_{g(\mathcal{X}) \rightarrow \infty} N(\mathcal{X})/g(\mathcal{X}) = A(q).$$

For $0 < \delta < 1/2 - 1/A(q)$, define two families of integers $\{n = N(\mathcal{X}) - 1\}_{\mathcal{X}}$ and $\{m = \lfloor \delta(N(\mathcal{X}) - 1) \rfloor + 2g\}_{\mathcal{X}}$. Then $n/g(\mathcal{X}) \rightarrow A(q)$ and $(m - 2g)/n \rightarrow \delta$.

By Proposition 3.4, from each curve $\mathcal{X}$ in the family we can construct a q -ary $((n, K = q^{n-2m+2g-2}, d = m - 2g + 2))$ -quantum code. Thus,

$$\frac{d}{n} \rightarrow \delta, \quad \frac{\log_q K}{n} \rightarrow 1 - 2\delta - \frac{2}{A(q)}.$$

The proof is completed. $\square$

Remark 3.7: The bound (3.2) is better than the quantum Gilbert–Varshamov bound (3.1) in an interval for some large q . In particular, when q is a square prime power bigger than or equal to 19^2 , the bound (3.2) improves on the bound (3.1) in an interval around $(q^2 - 1)/(2q^2 - 1)$. For instance, for $q = 19^2$, the bound (3.2) improves on the bound (3.1) in the interval $(0.3515, 0.4445)$.

Finally, we combine the idea from [16] with Proposition 2.4 to obtain the following result.

Theorem 3.8: For a prime power q , one has

$$\alpha_q^Q(\delta) \geq 1 - 2\delta - \frac{2}{A(q)} + \log_q \left(1 + \frac{1}{q^3} \right). \quad (3.3)$$

Proof: Let $\{\mathcal{X}/\mathbb{F}_q\}$ be a family of curves such that $g(\mathcal{X}) \rightarrow \infty$ and

$$\limsup_{g(\mathcal{X}) \rightarrow \infty} N(\mathcal{X})/g(\mathcal{X}) = A(q).$$

For $0 < \delta < 1/2 - 1/A(q)$, define two families of integers $\{n = N(\mathcal{X}) - 1\}_{\mathcal{X}}$ and $\{m = \lfloor \delta(N(\mathcal{X}) - 1) \rfloor + 2g(\mathcal{X})\}_{\mathcal{X}}$. Then $n/g(\mathcal{X}) \rightarrow A(q)$ and $(m - 2g)/n \rightarrow \delta$.

Put

$$l = n - 2m + 2g - 2s - 2t - 2$$

$$s = \left\lfloor \frac{qn}{(q-1)(q^3+1)} \right\rfloor, \quad t = \left\lfloor \frac{n}{q^3+1} \right\rfloor.$$

For each curve $\mathcal{X}/\mathbb{F}_q$ in the family, let $P_0, P_1, \dots, P_n$ be $N(\mathcal{X}) = n + 1$ rational points of $\mathcal{X}$. Put $\mathcal{P} = \{P_1, \dots, P_n\}$ and $C = C_L(mP_0; \mathcal{P})$.

For a divisor $D = \sum_{i=1}^t m_i P_i$ with $m_i \geq 1$, consider the disjoint set

$$F_D((m+l)P_0) := \{x \in \mathcal{L}(D + (m+l)P_0) \mid v_{P_i}(x) = -m_i, \text{ for all } 1 \leq i \leq t\}.$$

Then using the Riemann–Roch theorem and the inclusion–exclusion principle, one can show that the cardinality of $F_D((m+l)P_0)$ is

$$|F_D((m+l)P_0)| = q^{m+l+s-g+1}(1-1/q)^t, \quad \text{with } s = \sum_{i=1}^t m_i = \deg(D)$$

if $l+m \geq 2g-1$ (see [16]).

Consider the set of functions

$$T = \bigcup_D F_D((m+l)P_0)$$

where D runs over all divisors of the form

$$D = \sum_{j=1}^t m_{i_j} P_{i_j}, \quad \text{with } 1 \leq i_j \leq n, m_{i_j} \geq 1 \text{ and } \deg D = s. \quad (3.4)$$

Then by [16], we have

$$|T| = q^{m+l-g+1+s} \left(1 - \frac{1}{q}\right)^t \cdot \binom{n}{t} \cdot \binom{s-1}{t-1}.$$

Let $x_1, \dots, x_K$ be K elements of T such that

- i) $x_i + \mathcal{L}(mP_0) \neq x_j + \mathcal{L}(mP_0)$ for any $1 \leq i \neq j \leq K$; and
- ii) for any $x \in T$, there exists some $1 \leq j \leq K$ satisfying $x - x_j \in \mathcal{L}(mP_0)$.

Then

$$K \geq |T|/|\mathcal{L}(mP_0)| = q^{l+s} \left(1 - \frac{1}{q}\right)^t \cdot \binom{n}{t} \cdot \binom{s-1}{t-1}.$$

For each $1 \leq i \leq K$, assume that $x_i \in F_{D_i}((m+l)P_0)$ for some D_i of the form (3.4) and define a vector $\mathbf{v}_i = (v_{i1}, \dots, v_{in}) \in \mathbb{F}_q^n$ by

$$v_{ij} = \begin{cases} x_i(P_j), & \text{if } P_j \notin \text{Supp}(D_i) \\ 0, & \text{if } P_j \in \text{Supp}(D_i). \end{cases}$$

For $\mathbf{c} \in C$, let $\mathbf{c} = (y(P_1), \dots, y(P_n))$ for a function $y \in \mathcal{L}(mP_0)$. Then for $1 \leq i \neq j \leq K$, $x_i - x_j + y$ is a nonzero function in $\mathcal{L}((m+l)P_0 + D_i + D_j)$. Consider the set

$$Z := \{P_k \mid P_k \notin \text{Supp}(D_i) \cup \text{Supp}(D_j) \text{ and } (x_i - x_j + y)(P_k) = 0\}.$$

Then $x_i - x_j + y \in \mathcal{L}((m+l)P_0 + D_i + D_j - \sum_{P \in Z} P)$, hence, $m+l+2s-|Z| \geq 0$. On the other hand, one has

$$\text{wt}(\mathbf{v}_i - \mathbf{v}_j + \mathbf{c}) \geq n - |Z| - 2t$$

and hence,

$$\text{wt}(\mathbf{v}_i - \mathbf{v}_j + \mathbf{c}) \geq n - m - l - 2s - 2t = m - 2g + 2.$$

Since $d(C^\perp) \geq m - 2g + 2$, by Proposition 2.4, we get a q -ary $((n, K, d))$ -quantum code with $d \geq m - 2g + 2$. It follows that

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{d}{n} &\geq \delta \\ \text{and} \\ \frac{\log_q K}{n} + 2 \times \frac{d}{n} &= \frac{1}{n} \left(n - 2g - s - 3t + 2 + t \log_q(q-1) + \log_q \left(\binom{n}{t} \binom{s-1}{t-1} \right) \right) \\ &\rightarrow 1 - \frac{2}{A(q)} - \frac{q}{(q-1)(q^3+1)} - \frac{3}{q^3+1} + \frac{\log_q(q-1)}{q^3+1} \\ &\quad - \left(\frac{1}{q^3+1} \log_q \left(\frac{1}{q^3+1} \right) + \frac{q^3}{q^3+1} \log_q \left(\frac{q^3}{q^3+1} \right) \right) \\ &\quad - \frac{q}{(q-1)(q^3+1)} \left(\frac{q-1}{q} \log_q \left(\frac{q-1}{q} \right) + \frac{1}{q} \log_q \left(\frac{1}{q} \right) \right) \\ &= 1 - \frac{2}{A(q)} + \log_q \left(1 + \frac{1}{q^3} \right) \\ &\quad \text{(see [16] for the details on this limit).} \end{aligned}$$

Thus, the proof is completed. $\square$

ACKNOWLEDGMENT

The authors are grateful to three anonymous referees for their invaluable suggestions and comments which greatly improved the paper.

REFERENCES

- [1] A. Ashikhmin and E. Knill, “Nonbinary quantum stabilizer codes,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.
- [2] A. Ashikhmin and S. Litsyn, “Upper Bounds on the Size of Quantum Codes,” quant-ph/9709049, Sep. 1997.
- [3] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, “Asymptotically good quantum codes,” *Phys. Rev. A*, vol. 63, no. 3, p. 032311, Mar. 2001.
- [4] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction via codes over $GF(4)$,” *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
- [5] H. Chen, S. Ling, and C. P. Xing, “Asymptotically good quantum codes exceeding the Ashikhmin–Litsyn–Tsfasman bound,” *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 2055–2058, Jul. 2001.
- [6] K. Q. Feng and Z. Ma, “A finite Gilbert–Varshamov bound for pure stabilizer quantum codes,” *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3323–3325, Dec. 2004.
- [7] K. Feng and C. P. Xing, “A New Construction of Quantum Error-Correcting Codes,” *Trans. Amer. Math. Soc.*, to be published.
- [8] A. S. Hedayet, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays*. New York: Springer-Verlag, 1999.
- [9] R. Matsumoto, “Improvement of the Ashikhmin–Litsyn–Tsfasman bound for quantum codes,” *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 2122–2124, Jul. 2002.
- [10] E. Knill, “Non-Binary Unitary Error Bases and Quantum Codes,” quant-ph/9608048, Aug. 1996.
- [11] —, “Group Representations, Error Bases and Quantum Codes,” quant-ph/9608049, Aug. 1996.
- [12] R. Matsumoto and T. Uyematsu, “Constructing quantum error-correcting codes for p^m -state systems from classical error-correcting codes,” *IEICE Trans. Fundamentals*, vol. E83-A, no. 10, pp. 1878–1883, 2000.
- [13] E. M. Rains, “Nonbinary quantum codes,” *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1827–1832, Sep. 1999.
- [14] —, “Quantum codes of minimal distance two,” *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 266–271, Jan. 1999.
- [15] A. M. Steane, “Multiple particle interference and quantum error correction,” in *Proc. Roy. Soc. London A*, vol. 452, 1996, pp. 2551–2577.
- [16] H. Stichtenoth and C. P. Xing, “Excellent nonlinear codes from algebraic function fields,” *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 4044–4046, Nov. 2005.
- [17] M. A. Tsfasman and S. G. Vlăduț, *Algebraic-Geometric Codes*. Amsterdam, The Netherlands: Kluwer, 1991.